SYSTEM AND METHOD FOR DISCOVERING COMPROMISED SECURITY DEVICES

Publication number: WO9919822
Publication date: 1999-04-22
Inventor: BIRDWELL KENNETH J; YACOBI YACOV
Applicant: MICROSOFT CORP (US)
Classification:
- international: ***G06F1/00; G06F21/00; H04L9/10; H04L9/32; H04N7/167; H04N7/173;*** **G06F1/00; G06F21/00; H04L9/10; H04L9/32; H04N7/167; H04N7/173;** (IPC1-7): G06F121/04
- european: H04N7/173C; G06F21/00N7D; H04N7/167D
Application number: WO1998US19352 19980916
Priority number(s): US19970949438 19971014

Also published as:
WO9919822 (A3)
EP1031206 (A3)
EP1031206 (A2)
EP1031206 (A0)

Cited documents:
XP002097845

Report a data error here

Abstract of **WO9919822**

A data delivery system has a content server or other mechanism for delivering encoded content to multiple authorized clients. The authorized clients are equipped with security devices having decoding capabilities to decode the content. Unauthorized clients are prevented from decoding the content because they are not supplied with the decoding capabilities. As part of the data delivery system, a traitor detection system is provided to discover an identity of an authorized client that has been compromised and is illicitly transferring decoding capabilities to unauthorized clients. The traitor detection system generates different decoding capabilities and creates an association file which relates the different decoding capabilities to different authorized clients. The decoding capabilities are traced to determine which of them is illicitly transferred to an illegitimate user. In the event that one of the decoding capabilities is illicitly transferred, the traitor detection system consults the association file to identify one or more of the authorized clients that were originally supplied with the illicitly transferred decoding capabilities. The identified set of clients includes the compromised client. The process is repeated for the identified set of clients with a new set of decoding capabilities to successively narrow the field of possible pirating clients, until the compromised security device is precisely pinpointed.

Data supplied from the ***esp@cenet*** database - Worldwide